DECENTRALIZED ACCESS CONTROL OF DATA STORED IN CLOUD USING KEY POLICY ATTRIBUTE BASED ENCRYPTION

[1]S.Seenu Iropia, [2] R.Vijayalakshmi

[1]PG Scholar Department of Information Technology, SRM University, ssiropia@gmail.com.

[2]Assistant Professor Department of Information Technology, SRM University.

ABSTRACT: *Cloud computing is a rising computing standard in which assets of the computing framework are given as a service over the Internet. As guaranteeing as it may be, this standard additionally delivers a lot of people new challenges for data security and access control when clients outsource sensitive data for offering on cloud servers, which are not inside the same trusted dominion as data possessors. In any case, in completing thus, these results unavoidably present a substantial processing overhead on the data possessor for key distribution and data administration when fine-grained data access control is in demand, and subsequently don't scale well. The issue of at the same time accomplishing fine-grainedness, scalability, and data confidentiality of access control really still remains uncertain. This paper addresses this open issue by, on one hand, characterizing and implementing access policies based on data qualities, and, then again, permitting the data owner to representative the majority of the calculation undertakings included in fine-grained data access control to un-trusted cloud servers without unveiling the underlying data substance. We accomplish this goal by exploiting and combining techniques of decentralized key policy Attribute Based Encryption (KP-ABE) . Extensive investigation shows that the proposed approach is highly efficient and secure.*

Keywords: *Access Control, Cloud Computing, Key Policy Attribute Based Encryption (KP-ABE)*

I. INTRODUCTION

Cloud computing is a promising computing model which currently has drawn far reaching consideration from both the educational community and industry. By joining a set of existing and new procedures from research areas, for example, Service-Oriented Architectures (SOA) and virtualization, cloud computing is viewed all things considered a computing model in which assets in the computing infrastructure are given as services over the Internet. It is a new business solution for remote reinforcement outsourcing, as it offers a reflection of interminable storage space for customers to have data reinforcements in a pay-as-you- go way [1]. It helps associations and government offices fundamentally decrease their financial overhead of data administration, since they can now store their data reinforcements remotely to third-party cloud storage suppliers as opposed to keep up data centers on their own. Numerous services like email, Net banking and so forth… are given on the Internet such that customers can utilize them from anyplace at any time. Indeed cloud storage is more adaptable, how the security and protection are accessible for the outsourced data turns into a genuine concern. The three points of this issue are availability, confidentiality and integrity.

To accomplish secure data transaction in cloud, suitable cryptography method is utilized. The data possessor must encrypt the record and then store the record to the cloud. Assuming that a third person downloads the record, they may see the record if they had the key which is utilized to decrypt the encrypted record. Once in a while this may be failure because of the technology improvement and the programmers. To overcome the issue there is lot of procedures and techniques to make secure transaction and storage.

Recently [2] addressed Anonymous authentication for data archiving to clouds. Anonymous authentication is the procedure of accepting the client without the details of the client. So the cloud server doesn't know the details of the client, which gives security to the clients to conceal their details from other clients of that cloud.

Security and privacy assurance in clouds are analyzed and tested by numerous researchers. [3] gives storage security utilizing Reed-Solomon eradication correcting codes. Utilizing homomorphic encryption, [4] the cloud gains cipher text and furnishes an encoded value of the result. The client has the capacity to translate the result; however the cloud does not comprehend what data it has worked on.

In this paper key policy Attribute Based Encryption scheme is used to control unauthorized access. In addition revocation scheme is used for time based file assured deletion.

II. RELATED WORK

Access control in clouds is gaining consideration on the grounds that it is imperative that just authorized clients have access to services. A colossal measure of data is constantly archived in the cloud, and much of this is sensitive data. Utilizing Attribute Based Encryption (ABE), the records are encrypted under a few access strategy furthermore saved in the cloud. Clients are given sets of traits and corresponding keys. Just when the clients have matching set of attributes, would they be able to decrypt the data saved in the cloud. [5][6] Studied the access control in health care.

Access control is likewise gaining imperativeness in online social networking where users store their personal data, pictures, films and shares them with selected group of users they belong. Access control in online social networking has been studied in [7].

The work done by [8] gives privacy preserving authenticated access control in cloud. Nonetheless, the researchers take a centralized methodology where a single key distribution center (KDC) disperses secret keys and attributes to all clients. Unfortunately, a single KDC is not just a single point of failure however troublesome to uphold due to the vast number of clients that are upheld in a nature's domain. The scheme In [9] uses a symmetric key approach and does not support authentication.

Multi-authority ABE principle was concentrated on in [10], which obliged no trusted power which requires each client to have characteristics from at all the KDCs.

In spite of the fact that Yang et al. [11] proposed a decentralized approach, their strategy does not confirm clients, who need to remain anonymous while accessing the cloud. Ruj et al. [12] proposed a distributed access control module in clouds. On the other hand, the approach did not provide client verification. The other weakness was that a client can make and store an record and different clients can just read the record. write access was not allowed to clients other than the originator.

Time-based file assured deletion, which is initially presented in [13], implies that records could be safely erased and remain forever difficult to reach after a predefined time. The primary thought is that a record is encrypted with an information key by the possessor of the record, and this information key is further encrypted with a control key by a separate key Manager.

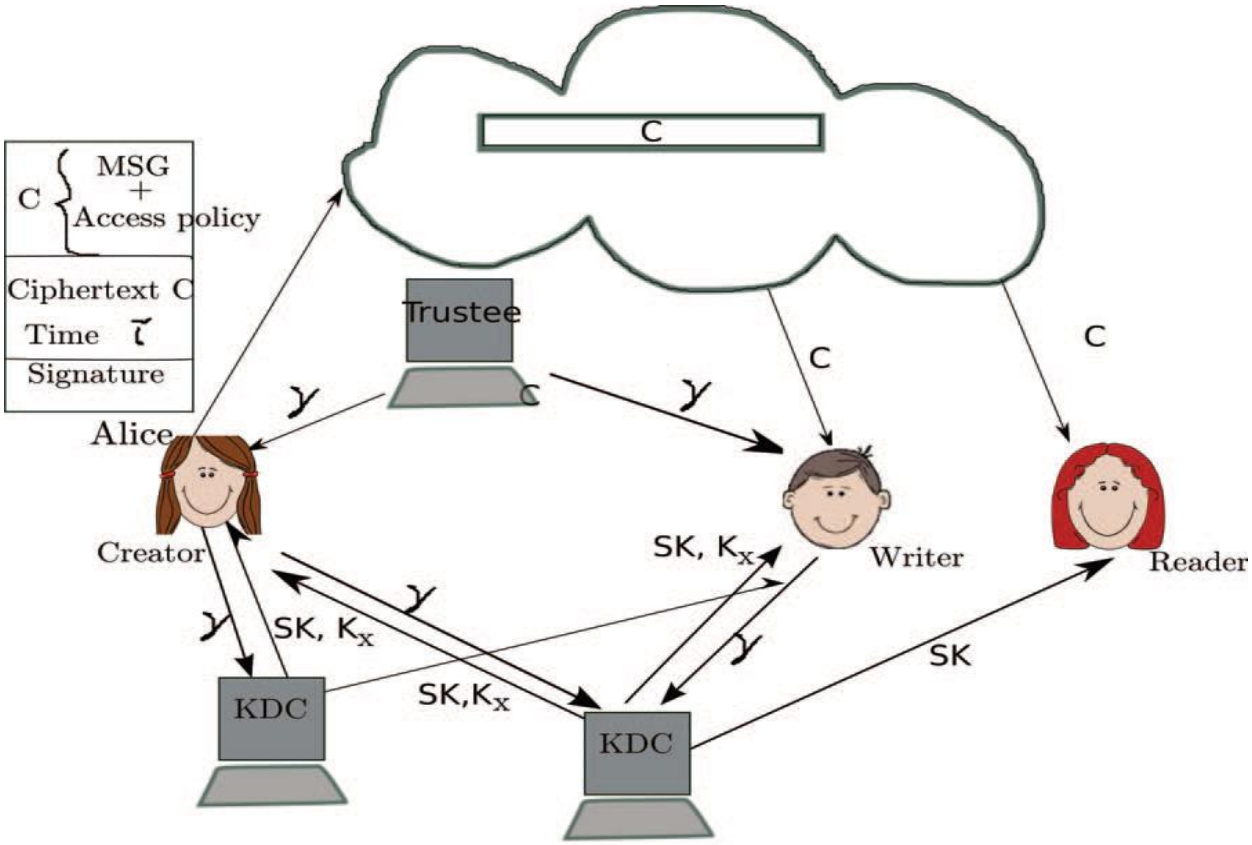

Fig 1 Cloud Architecture

III. PROPOSED METHODOLOGY

A. Distributed Key Policy Attribute Based Encryption

KP-ABE is a public key cryptography primitive for one-to-many correspondences. In KP-ABE, information is associated with attributes for each of which a public key part is characterized. The encryptor associates the set of attributes to the message by scrambling it with the comparing public key parts. Every client is assigned an access structure which is normally characterized as an access tree over information attributes, i.e., inside hubs of the access tree are limit doors and leaf hubs are connected with attributes. Client secret key is characterized to reflect the access structure so the client has the ability to decode a cipher-text if and just if the information attributes fulfill his access structure. The proposed scheme consists of four algorithms which is defined as follows

Setup:

This algorithm takes as input security parameters and attribute universe of cardinality N. It then defines a bilinear group of prime number. It returns a public key and the master key which is kept secret by the authority party.

Encryption:

It takes a message, public key and set of attributes. It outputs a cipher text.

Key Generation:

It takes as input an access tree, master key and public key. It outputs user secret key.

Decryption:
It takes as input cipher text, user secret key and public key. It first computes a key for each leaf node. Then it aggregates the results using polynomial interpolation technique and returns the message.

B. File Assured Deletion
The policy of a file may be denied under the request by the customer, when terminating the time of the agreement or totally move the files starting with one cloud then onto the next cloud nature's domain. The point when any of the above criteria exists the policy will be repudiated and the key director will totally evacuates the public key of the associated file. So no one can recover the control key of a repudiated file in future. For this reason we can say the file is certainly erased.

To recover the file, the user must ask for the key supervisor to produce the public key. For that the user must be verified. The key policy attribute based encryption standard is utilized for file access which is verified by means of an attribute connected with the file. With file access control the file downloaded from the cloud will be in the arrangement of read just or write underpinned. Every client has connected with approaches for each one file. So the right client will access the right file. For making file access the key policy attribute based encryption.

IV. CONCLUSION

We have introduced a decentralized access control system with anonymous authentication, which gives client renouncement also prevents replay attacks. The cloud does not know the identity of the client who saves data, however just checks the client's certifications. Key dissemination is carried out in a decentralized manner. One limit is that the cloud knows the access strategy for each one record saved in the cloud.

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A View of Cloud Computing. *Comm. of the ACM, 53(4):50–58, Apr 2010.*
2. Sushmita Ruj, Milos Stojmenovic and Amiya Nayak,"Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS.*
3. Wang, Q.Wang, K.Ren, N.Cao and W.Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", *IEEE T.Services Computing, Vol. 5, no.2, pp. 220-232, 2012.*
4. C.Gentry, "A fully homomorphic encryption scheme", *Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.*
5. personal M. Li, S. Yu, K. Ren, and W. Lou, "Securing health records in cloud computing: Patient-centric and fine-grained data access control in multi owner settings," in *SecureComm, pp. 89–106, 2010.*
6. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *ACM ASIACCS, pp. 261–270, 2010.*
7. S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation," in *ACM ASIACCS, 2011.*
8. F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in *ISPEC*, ser. Lecture Notes in Computer Science, *vol. 6672. Springer, pp. 83–97, 2011.*

9. W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in *ACM Cloud Computing Security Workshop (CCSW)*, 2009.
10. M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in *ACM Conference on Computer and Communications Security, pp. 121–130, 2009*.
11. Kan Yang, Xiaohua Jia and Kui Ren, " DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems", *IACR Cryptology ePrint Archive*, 419, 2012.
12. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in *IEEE TrustCom, 2011*.
13. . Perlman, "File System Design with Assured Delete," *Proc.Network and Distributed System Security Symp. ISOC (NDSS), 2007*.